AMENDMENTS TO THE CLAIMS

Please amend the claims as indicated hereafter. [Use ~~strikethrough~~ for deleted matter (or double square brackets "[[]]" if the strikethrough is not easily perceivable, *i.e.*, "4" or a punctuation mark) and underlined for added matter.]

1. (Currently amended) A document printout device for receiving and printing out digital documents, the printout device comprising:

a store of digital certificates, each certificate being associated with a received digital document and a sender of the received digital document; ~~and~~

an audit log comprising a list of received document entries, each entry containing a reference to one of the certificates in the store, an encrypted digest corresponding to the received digital document of that entry, and a unique identifier associated with [[a]] the received digital documents;

a decryption algorithm for decrypting the received encrypted digest associated with one of the received digital document selected for verification; and

a hash algorithm for creating a digest of the selected digital document such that when the created digest corresponds to the decrypted digest, the digital certificate of the sender is authenticated.

2. (Original) A device according to Claim 1, wherein the device is arranged to carry out an on-line authentication of a received certificate held in the store of received documents.

3. (Original) A device according to Claim 2, wherein the device is arranged to carry out a batch of on-line authentications of received certificates held in the store of received documents.

4. (Original) A device according to Claim 1, wherein each entry in the audit log contains a digest of the received document to which it relates.

5. (Original) A device according to Claim 4, further comprising a hash algorithm for creating a digest of a digital document and a receiving module for receiving a digital representation of a previously printed out document, wherein the device is

arranged to create a digest of the digital representation of the previously printed out document and to compare the newly created digest with the corresponding digest stored in the audit log.

6. (Original) A device according to Claim 5, wherein the device is arranged to send either a stored digest or a newly created digest of a document to its original sender and to verify the authenticity of the document back to its source by considering the transmitted results of a comparison of digests carried out at the source.

7. (Original) A device according to Claim 5, wherein the receiving module is a document scanning module.

8. (Original) A device according to Claim 1, wherein each entry in the audit log contains the time and date of receipt of each digital document.

9. (Original) A device according to Claim 1, wherein the unique identifier is an alphanumeric code and the device further comprises an input module for inputting the code to access the relevant entry in the audit log.

10. (Original) In a facsimile machine adapted for receiving and printing out digital documents, a device comprising:

a store of digital certificates, each certificate being associated with a received digital document; and

an audit log comprising a list of received document entries, each entry containing a reference to one of the certificates in the store and a unique identifier associated with a received digital document.

11. (Currently amended) A method of authenticating the identity of a sender of a received digital document, the method comprising:

using a unique identifier printed on the received document to search for a corresponding record in a list of received document records;

referencing a digital certificate associated with the selected record, the certificate being one of a store of certificates of received documents and each digital certificate being associated with a sender of the received digital document;

receiving an encrypted digest of the received digital document;

decrypting the encrypted digest;

computing a value of a second digest from the received digital document;

comparing the computed value of the second digest with a value of the decrypted digest; and

carrying out an on-line authentication of the certificate when the computed value of the second digest corresponds with the value of the decrypted digest.

12. (New) A device according to Claim 1, wherein each digital certificate comprises a public key associated with a sender of the received digital document; wherein the decryption algorithm decrypts the encrypted digest using the sender's public key extracted from the digital certificate; wherein the hash algorithm computes a digest of a document copy, and wherein authenticity of the copied document is verified when the computed digest corresponds to the decrypted digest.

13. (New) A device according to Claim 12, further comprising a remote device that encrypts the digest of the received digital document using the sender's private key.

14. (New) A method according to Claim 11, wherein the digital certificate comprises a public key associated with the sender of the received digital document and wherein the encrypted digest is encrypted with a private key of the sender, the method further comprising:

decrypting the encrypted digest using the public key of the sender extracted from the certificate.

15. (New) A method according to Claim 11, further comprising:

receiving a copy of a document;

computing a digest of the document copy;

comparing the computed digest with the decrypted digest; and

determining that the document copy is authentic when the computed digest corresponds to the decrypted digest.

16. (New) A method according to Claim 11, wherein computing the digest of the document copy further comprises using a hash algorithm to compute the digest of the document copy, wherein the hash algorithm is the same as an original hash algorithm used to originally generate the decrypted digest.